Sheet 1 of 3

Form PTO-1449 **INFORMATION DISCLOSURE CITATION IN AN APPLICATION** (Use several sheets if necessary)	ATTY DOCKET NO. 2925-161P	APPLICATION NO 09/127,767
	APPLICANT Sarvar PATEL	
	FILING DATE July 31, 1998	GROUP 2744

U.S. PATENT DOCUMENTS

EXAMINER INITIAL	DOCUMENT NUMBER							DATE	NAME	CLASS	SUB CLASS	FILING DATE IF APPROPRIATE
SK	5	1	5	3	9	1	9	10/06/1992	Reeds, III et al.			

FOREIGN PATENT DOCUMENTS

	DOCUMENT NUMBER							DATE	COUNTRY	CLASS	SUB CLASS	TRANSLATION	
												YES	NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, etc.)

SK		M. Bellare and P. Rogaway, Entity authentication and key distribution, *Advances in Cryptology - Crypto*, 1993.
		S. Bellovin and M. Merritt, Encrypted key exchange: password-based protocols secure against dictionary attacks, *IEEE computer society symposium on research in security and privacy*, 72-84 May 1992.
		R. Bird, I. Gopal, A. Herzberg, P. Janson, S. Kutten, R. Molva, and M. Yung, Systematic design of two-party authentication protocols, *Advances in Cryptology - Crypto*, 1991.
		M. Blum and S. Micali, How to generate cryptographically strong sequences of pseudo random bits, *SIAM J. Computing*, 13 No. 4:850-864, 1984.
		R. B. Boppana and R. Hirschfeld, Pseudorrandom generators and complexity classes, *Advances in Computing Research*, 5 (S. Micali, Ed.), JAI Press, CT.
		U.S. Department of Commerce/N.I.S.T., *Digital Signature Standard*, FIPS 186, May 1994.
		O. Goldreich and L. A. Levin, A hard-core predicate for all one way functions, *Proceedings of 21st STOC*, 25-32, 1989.
		S. Goldwasser and A. Micali, Probabilistic encryption, *Journal of Computer and Systems Science*, 28: 270-299, 1984.
		L. Gong, T. Lomas, R. Needham and J. Saltzer, Protecting poorly chosen secrets from guessing attacks, *IEEE Journal on Selected Areas in Communications*, 11(5): 648-656, June 1993.
		EIA/TIA, Cellular RadioTelecommunications Intersystem Operations IS-41 Rev. D, 1997.

EXAMINER	DATE CONSIDERED 11/21/00

EXAMINER: Initial if citation considered, whether or not citation is in conformance with M.P.E.P. 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Sheet 2 of 3

Form PTO-1449 **INFORMATION DISCLOSURE CITATION IN AN APPLICATION** (Use several sheets if necessary)	ATTY DOCKET NO. 2925-161P	APPLICATION NO 09/127,767
	APPLICANT Sarvar PATEL	
	FILING DATE July 31, 1998	GROUP 2744

U.S. PATENT DOCUMENTS

EXAMINER INITIAL	DOCUMENT NUMBER	DATE	NAME	CLASS	SUB CLASS	FILING DATE IF APPROPRIATE

FOREIGN PATENT DOCUMENTS

	DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUB CLASS	TRANSLATION	
						YES	NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, etc.)

SK		T. Lomas, L. Gong, J. Saltzer and R. Needham, Reducing Risks from Poorly Chosen Keys, *Proceedings of the 12th ACM Symposium on Operating System Principles*, *ACM Operating Systems Review*, 23(5): 14-18, December 1989.
		S. Patel, Information Leakage in Encrypted Key Exchange, *Proceedings of DIMACS workshop on Network Threats*, 38: 33-40, December 1996.
		S. Patel, Number theoretic attacks on secure password schemes, *IEEE symposium on security and privacy*, 236-247, May 1997.
		S. Patel, Weaknesses of the north american wireless authentication protocol, *IEEE Personal Communications*, 40-44, June 1997.
		A. C. Yao, Theory and applications of trapdoor functions, *Proceedings of 23rd FOCS*, 80-91, 1982.
		M. Beller, L. Chang and Y. Yacobi, Privacy and authentication on a portable communication system, *IEEE J. Selected Areas in Communications*, 11(6): 821-829, 1993.
		C. Carroll, Y. Frankel and Y. Tsiounis, Efficient key distribution for slow computing devices: Achieving fast over the air activation for wireless systems, *IEEE symposium on security and privacy*, May 1998.
		TIA/EIA Interim Standard, *Over-the Air Service Provisioning of Mobile Stations in Spread Spectrum Systems*, IS-683-A, June 1998.
		E. Blossom, The VPI Protocol for Voice Privacy Devices, December 1996.
		O. Goldreich, S. Goldwasser and A. Micali, On the cryptographic applications of random functions, *Advances in Cryptology - Crypto*, 1984.
		D. Jablon, Strong Password-Only Authenticated Key Exchange, *ACM SIG-COMM Computer Communications Review*, October 1996.

EXAMINER	DATE CONSIDERED 11/21/00

EXAMINER: Initial if citation considered, whether or not citation is in conformance with M.P.E.P. 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Sheet 3 of 3

Form PTO-1449

INFORMATION DISCLOSURE CITATION IN AN APPLICATION

(Use several sheets if necessary)

ATTY DOCKET NO. 2925-161P	APPLICATION NO 09/127,767
APPLICANT Sarvar PATEL	
FILING DATE July 31, 1998	GROUP 2744

U.S. PATENT DOCUMENTS

EXAMINER INITIAL	DOCUMENT NUMBER	DATE	NAME	CLASS	SUB CLASS	FILING DATE IF APPROPRIATE

FOREIGN PATENT DOCUMENTS

	DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUB CLASS	TRANSLATION	
						YES	NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, etc.)

	SK	S. Lucks, Open Key Exchange: How to defeat dictionary attacks without encrypting public keys, Proceedings of the Security Protocol Workshop '97, 1997.
	SK	Oded Goldreich, Shafi Goldwasser, Silvio Micali, How to Construct Random Functions, Journal of the Association for Computing Machinery, Vol. 33, No. 4, pp. 792-807, October 1986.

EXAMINER	DATE CONSIDERED 11/21/00

EXAMINER: Initial if citation considered, whether or not citation is in conformance with M.P.E.P. 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.